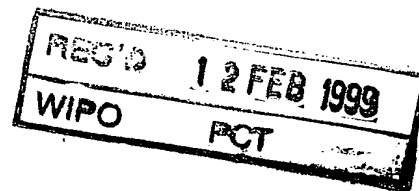


DE 98/03431

**PRIORITY  
DOCUMENT**

SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)



**Bescheinigung**

Die ROBERT BOSCH GMBH in Stuttgart/Deutschland hat eine  
Patentanmeldung unter der Bezeichnung

"System zur Kontrolle der Zugangsberechtigung"

am 11. Dezember 1997 beim Deutschen Patent- und Markenamt  
eingereicht.

Die angehefteten Stücke sind eine richtige und genaue  
Wiedergabe der ursprünglichen Unterlagen dieser Patent-  
anmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vor-  
läufig die Symbole E 05 B, G 07 C und B 60 R der Interna-  
tionalen Patentklassifikation erhalten.

München, den 8. Dezember 1998  
Deutsches Patent- und Markenamt  
Der Präsident  
Im Auftrag

Zeichen: 197 55 092.4

Ebert

28.11.97 Lc/Dn

5

ROBERT BOSCH GMBH, 70442 Stuttgart

10

System zur Kontrolle der Zugangsberechtigung

Stand der Technik

15

Die Erfindung geht aus von einem System zur Kontrolle der Zugangsberechtigung nach der Gattung des unabhängigen Anspruchs. Aus der DE 44 28 947 C1 ist bereits eine Schließvorrichtung für ein Kraftfahrzeug mit einer Betätigungseinrichtung sowie mit einem Transponder bekannt.

20

Bei Betätigung eines Senders ist ein Fernbetätigungswechselcodewort erzeugbar, das eine Decodiereinrichtung empfängt, mit einem in der Decodiereinrichtung gespeicherten Fernbetätigungswechselcodesignal vergleicht und in Abhängigkeit von dem Vergleich ein Entriegelungssignal erzeugt. Zur Erhöhung der Sicherheit ist darüberhinaus ein Transponder vorgesehen, dessen Wechselcodesignal zusätzlich für eine Freigabe ausgewertet wird.

30

Der Erfindung liegt die Aufgabe zugrunde, obengenanntes System zu vereinfachen, ohne einen Sicherheitsverlust zu erleiden. Die Aufgabe ist durch die kennzeichnenden Merkmale des unabhängigen Anspruchs gelöst.

Das erfindungsgemäße System zur Kontrolle der  
Zugangsberechtigung umfaßt ein Basisgerät, das ein Codewort  
empfängt. Das Codewort enthält eine Response, die ein  
Rechner mit einer Sollresponse vergleicht. Eine  
5 Zugangsberechtigung erfolgt bei Übereinstimmen von Response  
und Sollresponse. Zumindest eine Fernbedienung sendet das  
Codewort. Das erfindungsgemäße System zeichnet sich dadurch  
aus, daß in der Fernbedienung eine vom Basisgerät gesendete  
Challenge gespeichert ist zur Generierung des Codeworts.  
10 Diese Challenge ist identisch mit derjenigen eines bereits  
in der Vergangenheit erfolgreich durchgeführten Challenge-  
Response-Verfahrens. Die Challenge gibt somit einen Hinweis  
auf eine Berechtigung der Fernbedienung. Dadurch werden  
Manipulationsmöglichkeiten eingeschränkt. Andererseits ist  
15 für den Start einer Zugangsberechtigungsprozedur ein  
erneutes bidirektionales Challenge-Response-Verfahren nicht  
mehr notwendig, da die Challenge bereits in dem Speicher der  
Fernbedienung hinterlegt ist. Auf diese Weise läßt sich das  
Codewort bereits mit einer größeren Reichweite an das  
20 Basisgerät senden, während die Challenge-Response-Prozedur  
nur im Nahbereich durchgeführt werden kann. Damit ist eine  
Entkopplung zwischen bidirektionaler Datenübertragung und  
unidirektionaler Datenübertragung gewährleistet. In der  
Fernbedienung ist lediglich ein Sender größerer Reichweite  
vorzusehen, nicht jedoch ein entsprechender Empfänger für  
den Fernbereich. Die Challenge kann zur Synchronisation  
zwischen Basisgerät und Fernbedienung verwendet werden.  
Zudem sind weder im Basisgerät noch in der Fernbedienung die  
für die Zugangsberechtigung unmittelbar maßgebliche Response  
30 bzw. Sollresponse abgespeichert, so daß der direkte Zugriff  
auf diese sicherheitsrelevanten Informationen nicht möglich  
ist.

In einer zweckmäßigen Weiterbildung ist die Sollresponse in  
35 Abhängigkeit von einer in der Fernbedienung hinterlegten und

im Codewort enthaltenen Kennung gebildet. Dadurch wird eine eindeutige Zuordnung zwischen der verwendeten Fernbedienung und der zugehörigen, im Basisgerät abgelegten Verschlüsselung erreicht. Die eindeutige Zuordnung gewährleistet eine hinreichend hohe Sicherheit gegen unberechtigte Manipulationsversuche. Dadurch kann der Algorithmus, der in der Fernbedienung die gespeicherte Challenge - beispielsweise unter Verwendung einer fernbedienungsspezifischen Kennung - zu einer Response verschlüsselt, einfach ausfallen und in einem Mikrocontroller integriert sein.

In einer Ausgestaltung wird die im Basisgerät hinterlegte Challenge nach einer vorgegebenen Zahl fehlender Übereinstimmungen von Response und Sollresponse gelöscht. Damit ist bei einer Anzahl mißlungender Öffnungsversuche gewährleistet, daß eine Zugangsberechtigung bei weiterem Probieren nicht mehr erfolgt. Ein erneuter Öffnungsversuch ist nur in Verbindung mit einem erfolgreich durchlaufenden Challenge-Response-Verfahren zuzulassen. Bei Scheitern der Zugangsberechtigung über das unidirektionale Protokoll werden die Sicherheitsanforderungen erhöht, indem ein Zugang nur in Verbindung mit dem komplexen bidirektionalen Protokoll erreicht werden kann.

Eine vorteilhafte Ausgestaltung sieht vor, daß im Codewort ein Zählercode enthalten ist, der von dem Basisgerät mit einem Referenzcode verglichen wird. Nur bei einer Abweichung erfolgt eine Zugangsberechtigung. Der Zählercode wird mit der Betätigung eines Bedienelements der Fernbedienung verändert. Ein Senden des eben abgehörten Codeworts löst keine Zugangsberechtigung aus. Im Codewort kann der Zählerstand sowohl unverschlüsselt als auch verschlüsselt vorhanden sein.

Als Referenzcode ist ein gesendeter Code verwendet. Eine separate Zählerfunktion im Basisgerät ist hierfür nicht vorzusehen.

5       Zweckmäßig erfolgt die Übertragung des Codeworts hochfrequent und die Übertragung der Challenge niederfrequent. Aufgrund der gespeicherten Challenge benötigt die Fernbedienung keinen Empfänger im Hochfrequenzbereich.

10       Weitere zweckmäßige Weiterbildungen ergeben sich aus weiteren abhängigen Ansprüchen und aus der Beschreibung.

#### Zeichnung

15       Zwei mögliche Ausführungsbeispiele eines erfindungsgemäßen Systems zur Kontrolle der Zugangsberechtigung sind in der Zeichnung dargestellt und in der nachfolgenden Beschreibung näher erläutert. Es zeigen die Figuren 1 und 2 ein  
20       Blockschaltbild und eine Zugangsberechtigungsprozedur eines ersten Ausführungsbeispiels, die Figuren 3 und 4 ein Blockschaltbild und eine Zugangsberechtigungsprozedur eines zweiten Ausführungsbeispiels.

#### Beschreibung

Mehrere Fernbedienungen F1, ... Fx, ... Fn kommunizieren mit einem Basisgerät BG, das einen Sender/Empfänger 12 und einen Rechner 16 umfaßt. Der Rechner 16 tauscht Daten aus mit dem  
30       Sender/Empfänger 12 und hat Zugriff auf im Speicher hinterlegten Challenges C1, ... Cx, ... Cn, Kennungen K1, ..., Kx, ... Kn und einen Grenzwert G. Exemplarisch ist der Aufbau der x-ten Fernbedienung Fx gezeigt. Ein Fernbedienungsrechner 20 hat Zugriff auf die im Speicher  
35       hinterlegte Kennung Kx und Challenge Cx. Er gibt Daten an

den Sender 22 ab und tauscht Daten aus mit einem Fernbedienungs-Sender/Empfänger 26. Der von einem Bedienelement 24 beeinflusste Signalzustand ist dem Fernbedienungsrechner 20 zugeführt.

5

Das zweite Ausführungsbeispiel gemäß Figur 3 unterscheidet sich von dem ersten Ausführungsbeispiel gemäß Figur 1 dadurch, daß in dem Basisgerät BG anstelle des Grenzwerts G ein Speicher für einen Referenzcode RZ1, ... RZx, ... RZn vorgesehen ist. Die Fernbedienung Fx weist ein zusätzliches Feld für einen Zählercode Zx auf.

10

Im folgenden wird die Funktionsweise des in Figur 1 dargestellten ersten Ausführungsbeispiels näher erläutert.

15

In dem Basisgerät BG ist für jede Fernbedienung F1, ... Fx, ... Fn eine entsprechende Kennung K1, ... Kx, ... Kn

hinterlegt. Dadurch kann das Basisgerät BG jede einzelne Fernbedienung Fx bzw. jede Fernbedienungsgruppe Fx - wenn beispielsweise einer Kennung Kx mehrere Fernbedienungen Fx zugeordnet sind - eindeutig identifizieren. Diese Kennungen K1, ... Kx, ... Kn können die entsprechenden Speicherplätze

20

sein beziehungsweise anhand des Speicherplatzes erkannt werden. Im Challenge-Response-Verfahren sendet das Basisgerät die Challenge Cx an die durch die Kennung Kx eindeutig zugeordnete Fernbedienung Fx. Ein Zufallsgenerator erzeugt diese Challenge Cx. Der Rechner 16 speichert die gesendete Challenge Cx in einem über die Kennung Kx adressierten Speicherplatz. Der Fernbedienungsrechner 20 legt die vom Basisgerät BG zuletzt gesendete Challenge Cx in

30

Der Benutzer startet die unidirektionale Kommunikation der Fernbedienung Fx mit dem Basisgerät BG, indem er das Bedienelement 24 betätigt, Schritt 101. Der Fernbedienungsrechner 20 verknüpft die im Speicher

35

hinterlegte Challenge Cx unter Verwendung einer für die  
spezielle Fernbedienung Fx fernbedienungsspezifischen  
Information mit einem Algorithmus, woraus die Response Rx  
entsteht. Als fernbedienungsspezifische Information ist  
5 beispielsweise ein Teil der Kennung Kx, ein in der  
Fernbedienung Fx fest hinterlegter Herstellercode verwendet.  
Wesentlich ist jedoch, daß diese Verschlüsselung, das heißt  
Algorithmus und fernbedienungsspezifische Informationen, der  
Challenge Cx für jede Fernbedienung Fx auch im Basisgerät BG  
10 bekannt und hinterlegt ist. In dem Codewort CWx sind die  
Kennung Kx und die Response Rx, gegebenenfalls entsprechende  
Aufweck- und Aktionsbefehle, enthalten. Der Sender 22 sendet  
das Codewort CWx an das Basisgerät BG, Schritt 103. Der  
Rechner 16 filtert aus dem empfangenen Codewort CWx die  
15 Kennung Kx. Der Rechner 16 wählt die mit dieser Kennung Fx  
adressierte Challenge Cx und Verschlüsselung aus, mit denen  
auch in der Fernbedienung Fx die Response Rx ermittelt  
wurde. Der Rechner 16 berechnet aus der im Basisgerät BG  
hinterlegten Challenge Cx, dem Algorithmus und der  
20 fernbedienungsspezifischen Information, also der  
Verschlüsselung, die Sollresponse Sx, Schritt 105. Im  
Basisgerät BG werden empfangene Response Rx und berechnete  
Sollresponse Sx verglichen, Schritt 107. Bei Übereinstimmung  
gibt der Rechner 16 ein entsprechendes Freigabesignal,  
Schritt 109. Andernfalls folgt die Abfrage 111, ob die  
Anzahl der mißlungenen Öffnungsversuche M bereits einen  
vorgebbaren Grenzwert G überschritten hat. Ist dies der  
Fall, wird kein weiterer Öffnungsversuch zugelassen, Schritt  
113. Zudem wird die im Basisgerät BG gespeicherte Challenge  
Cx gelöscht. Eine Zugangsberechtigung kann somit nur durch  
30 einen erfolgreichen Durchlauf der bidirektionalen Challenge-  
Response-Prozedur, nicht jedoch mit dem beschriebenen  
unidirektionalen Protokoll erreicht werden. Hat die Anzahl  
der mißlungenen Öffnungsversuche M den Grenzwert G noch  
35 nicht überschritten, wird die Anzahl M inkrementiert,

Schritt 115. Hieran schließt sich Schritt 105 an, das weitere Vorgehen läuft ab wie bereits beschrieben.

Die Schritte ab 111 erhöhen die Sicherheit der unidirektionalen Datenübertragung, sind jedoch nicht unbedingt erforderlich.

Das im folgenden beschriebene zweite Ausführungsbeispiel bezieht sich auf die Figuren 3 und 4. Wie bereits für das erste Ausführungsbeispiel ausgeführt, ist in der Fernbedienung Fx die Challenge Cx gespeichert. In der Fernbedienung Fx ist ein Zählercode Zx gespeichert, der bei Betätigung des Bedienelements 24 inkrementiert wird. Für jede Fernbedienung Fx ist in dem Basisgerät BG der zuletzt gesendete Zählercode Zx als Referenzcode RZ1, ... RZx, ... RZn hinterlegt. Nach Auslösen des Startvorgangs durch Betätigen des Bedienelements 24, Schritt 121, wird in Übereinstimmung mit dem ersten Ausführungsbeispiel die Response Rx berechnet. Der Zählercode Zx wird um Eins erhöht. In dem Codewort CWx ist neben der Response Rx und der Kennung Kx der Zählercode Zx verschlüsselt enthalten. Der Sender 22 sendet das Codewort CWx an den Sender/Empfänger 12, Schritt 123. Wiederum filtert der Rechner 16 aus dem empfangenen Codewort CWx die Kennung Kx, anhand derer er den der Fernbedienung Fx zugehörigen Referenzcode RZx ausliest, Schritt 125. Nachfolgend wird der Zählercode Zx mit dem Referenzcode RZx verglichen, Schritt 127. Da in dem Basisgerät BG der zuletzt gesendete Zählercode Zx als Referenzcode RZx gespeichert ist, weichen bei einer ordnungsgemäßen Betätigung der Fernbedienung Fx Zählercode Zx und Referenzcode RZx voneinander ab. Stimmen sie jedoch überein, wird abgebrochen, Schritt 129. Eine Zugangsberechtigung erfolgt nicht. Andernfalls ermittelt das Basisgerät BG wie bereits für das erste Ausführungsbeispiel, die Sollresponse Sx, Schritt 131. Stimmen Response Rx und



Sollresponse Sx nicht überein, Schritt 133, so wird abgebrochen, Schritt 135. Andernfalls wird die Berechtigung zur Einleitung eines Öffnungsvorgangs gegeben, Schritt 137.

5 Als alternatives zweites Ausführungsbeispiel wird der Zählercode Zx in der Fernbedienung Fx verschlüsselt. Zur Ermittlung des Referenzcodes RZx ist diese Verschlüsselung adressiert im Basisgerät BG abzulegen. Für den Zählercode Zx ist nur von Bedeutung, daß er sich mit jeder Betätigung der Fernbedienung fx verändert, ob durch eine Zählerfunktion  
10 oder einen sonstigen Algorithmus, ist nicht wesentlich.

Die beiden Ausführungsbeispiele lassen sich auch dahingehend kombinieren, daß beispielsweise im Ablauf gemäß Figur 4 die  
15 Abfrage nach Schritt 111 durchgeführt wird. Dadurch läßt sich die Sicherheit gegenüber unberechtigten Öffnungsversuchen weiter erhöhen.

20 Die nicht näher ausgeführte Challenge-Response-Prozedur erfolgt vorzugsweise niederfrequent im Nahbereich des zu betretenden Raumes, beispielsweise ein Kraftfahrzeug. Der Sender 22 hingegen sendet ein höherfrequentes Signal, das eine größere Reichweite zuläßt. Ein Empfänger im höherfrequenten Bereich ist für die Fernbedienung Fx nicht vorzusehen. Der Algorithmus zur Verschlüsselung der Challenge Cx, um die Response Rx zu erhalten, ist vorzugsweise so einfach auszuführen, daß dieser auch in einem Mikrocontroller implementiert werden kann.

28.11.97 Lc/Dn

ROBERT BOSCH GMBH, 70442 Stuttgart

5

### Ansprüche

10

1. System zur Kontrolle der Zugangsberechtigung,  
- mit einem Basisgerät (BG), das ein Codewort (CWx)  
empfängt, das eine Response (Rx) enthält, die ein Rechner  
(16) mit einer Sollresponse (Sx) vergleicht, wobei eine  
Zugangsberechtigung bei Übereinstimmen von Response (Rx) und  
Sollresponse (Sx) erfolgt,

15

- mit zumindest einer Fernbedienung (F1, ... Fx, ... Fn),  
die das Codewort (CWx) sendet, dadurch gekennzeichnet, daß  
in der Fernbedienung (F1, ... Fx, ... Fn) eine vom  
Basisgerät (BG) gesendete Challenge (Cx) gespeichert ist zur  
Generierung des Codeworts (CWx).

20

2. System nach Anspruch 1, dadurch gekennzeichnet, daß die  
Sollresponse (Sx) in Abhängigkeit von einer in der  
Fernbedienung (F1, ... Fx, ... Fn) hinterlegten und im  
Codewort (CWx) enthaltenen Kennung (K1, ... Kx, ... Kn)  
gebildet ist.

30

3. System nach einem der vorhergehenden Ansprüche, dadurch  
gekennzeichnet, daß die Challenge (Cx) in dem Basisgerät  
(BG) gespeichert ist.

4. System nach einem der vorhergehenden Ansprüche, dadurch  
gekennzeichnet, daß die im Basisgerät (BG) hinterlegte  
Challenge (Cx) dann gelöscht ist, wenn die Anzahl fehlender

Übereinstimmung von Response (Rx) und Sollresponse (Sx)  
einen vorgebbaren Grenzwert (G) übersteigt.

5 5. System nach einem der vorhergehenden Ansprüche, dadurch  
gekennzeichnet, daß im Codewort (CWx) ein Zählercode (Zx)  
enthalten ist, der von dem Basisgerät (BG) mit einem  
Referenzcode (RZx) verglichen ist.

10 6. System nach einem der vorhergehenden Ansprüche, dadurch  
gekennzeichnet, daß der Zählercode (Zx) bei Betätigung eines  
Bedienelements (24) der Fernbedienung (F), ... Fx, ... Fn)  
verändert ist.

15 7. System nach einem der vorhergehenden Ansprüche, dadurch  
gekennzeichnet, daß als Referenzcode (RZx) ein gesendeter  
Zählercode (Zx) verwendet ist.

20 8. System nach einem der vorhergehenden Ansprüche, dadurch  
gekennzeichnet, daß der Zählercode (Zx) verschlüsselt in dem  
Codewort (CWx) enthalten ist.

9. System nach einem der vorhergehenden Ansprüche, dadurch  
gekennzeichnet, daß die Übertragung des Codeworts (CWx)  
hochfrequent und die Übertragung der Challenge (Cx)  
niederfrequent erfolgt.

28.11.97 Lc/Dn

ROBERT BOSCH GMBH, 70442 Stuttgart

5

System zur Kontrolle der Zugangsberechtigung

10

Zusammenfassung

15

Es wird ein System zur Kontrolle der Zugangsberechtigung vorgeschlagen. Es umfaßt ein Basisgerät (BG), das ein Codewort (CWx) empfängt, das eine Response (Rx) enthält. Ein Rechner (16) vergleicht die Response (Rx) mit einer Sollresponse (Sx). Eine Zugangsberechtigung erfolgt bei Übereinstimmen von Response (Rx) und Sollresponse (Sx). Eine Fernbedienung (F1, ... Fx, ... Fn) sendet das Codewort (CWx). Das System zeichnet sich dadurch aus, daß in der Fernbedienung (F1, ... Fx, ... Fn) eine vom Basisgerät (BG) gesendete Challenge (Cx) gespeichert ist zur Generierung des Codeworts (CWx).

20

1 / 4

Fig. 1

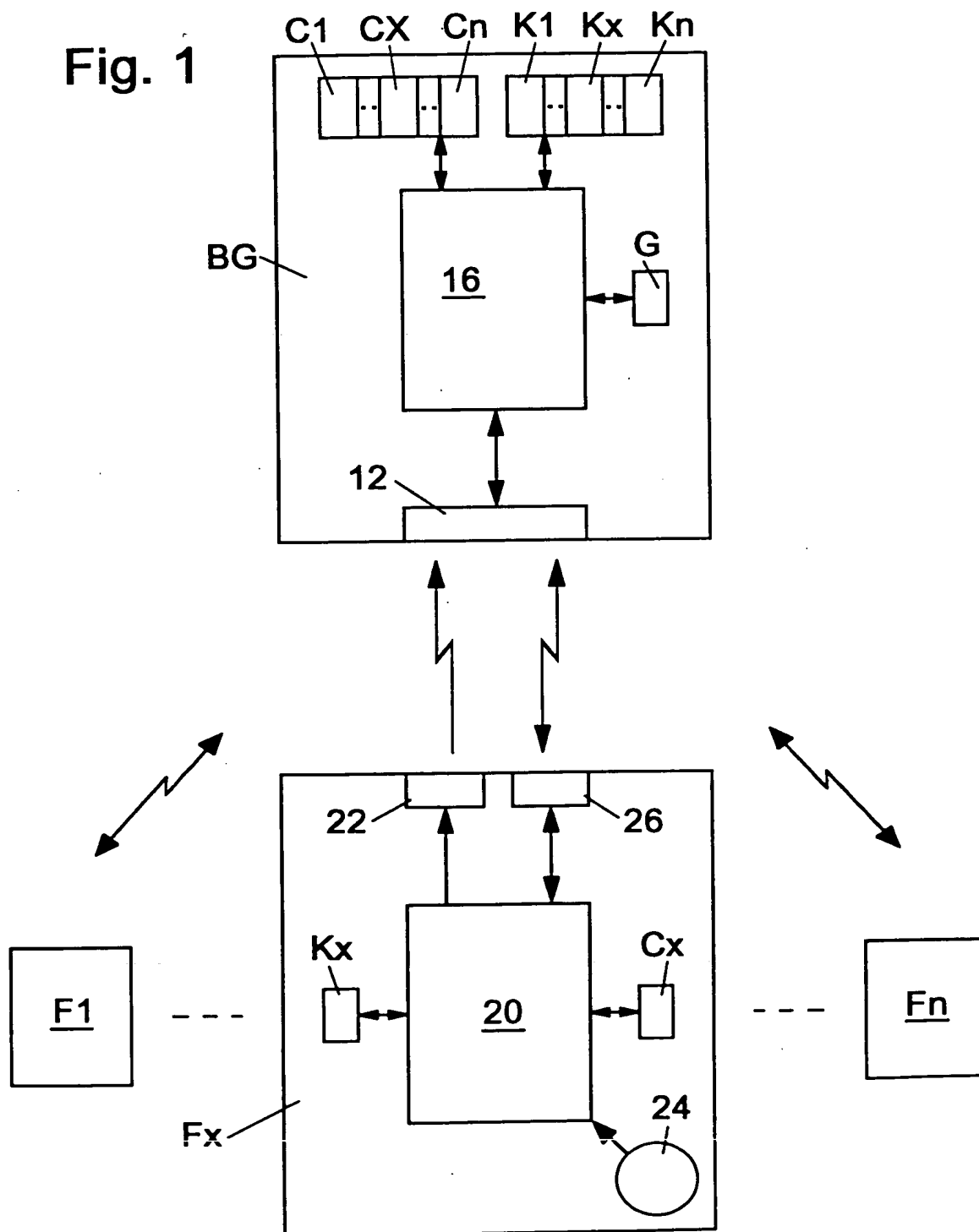
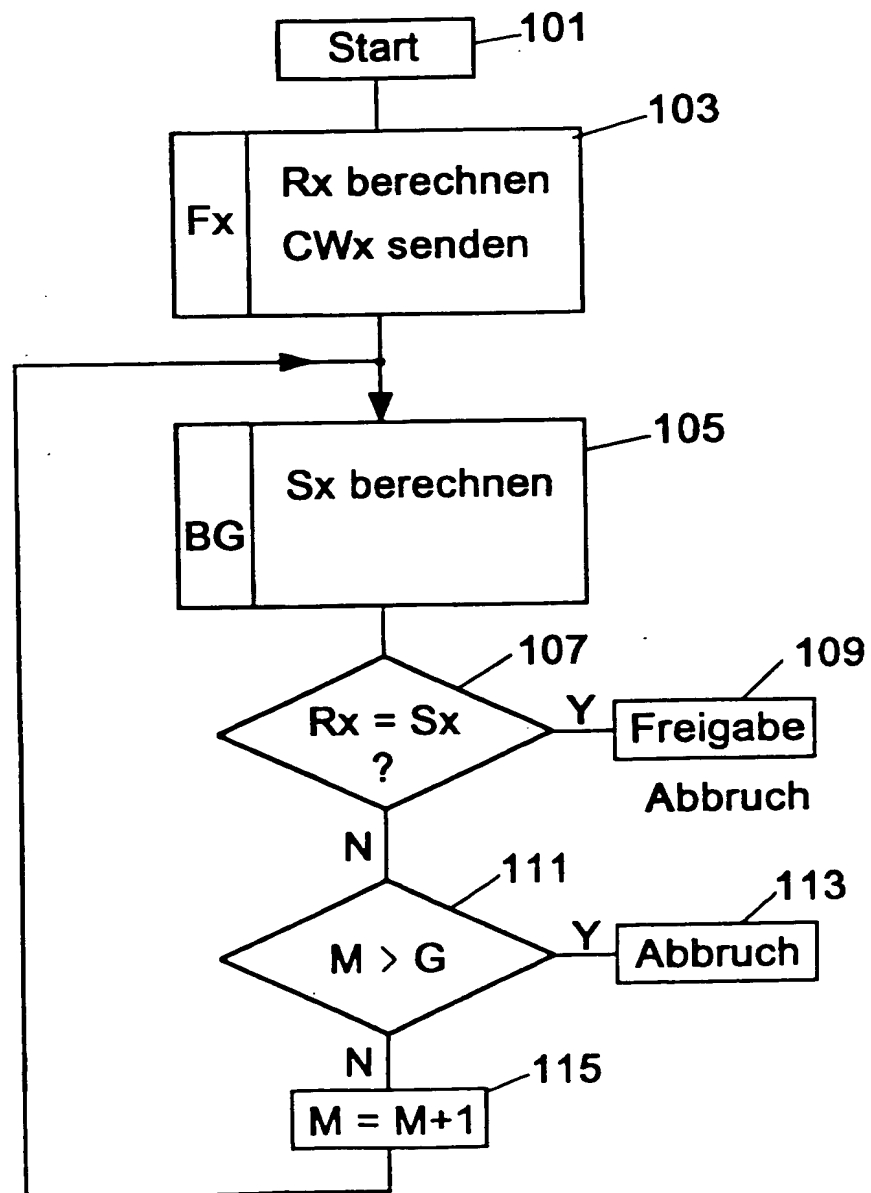


Fig. 2



3 / 4

Fig. 3

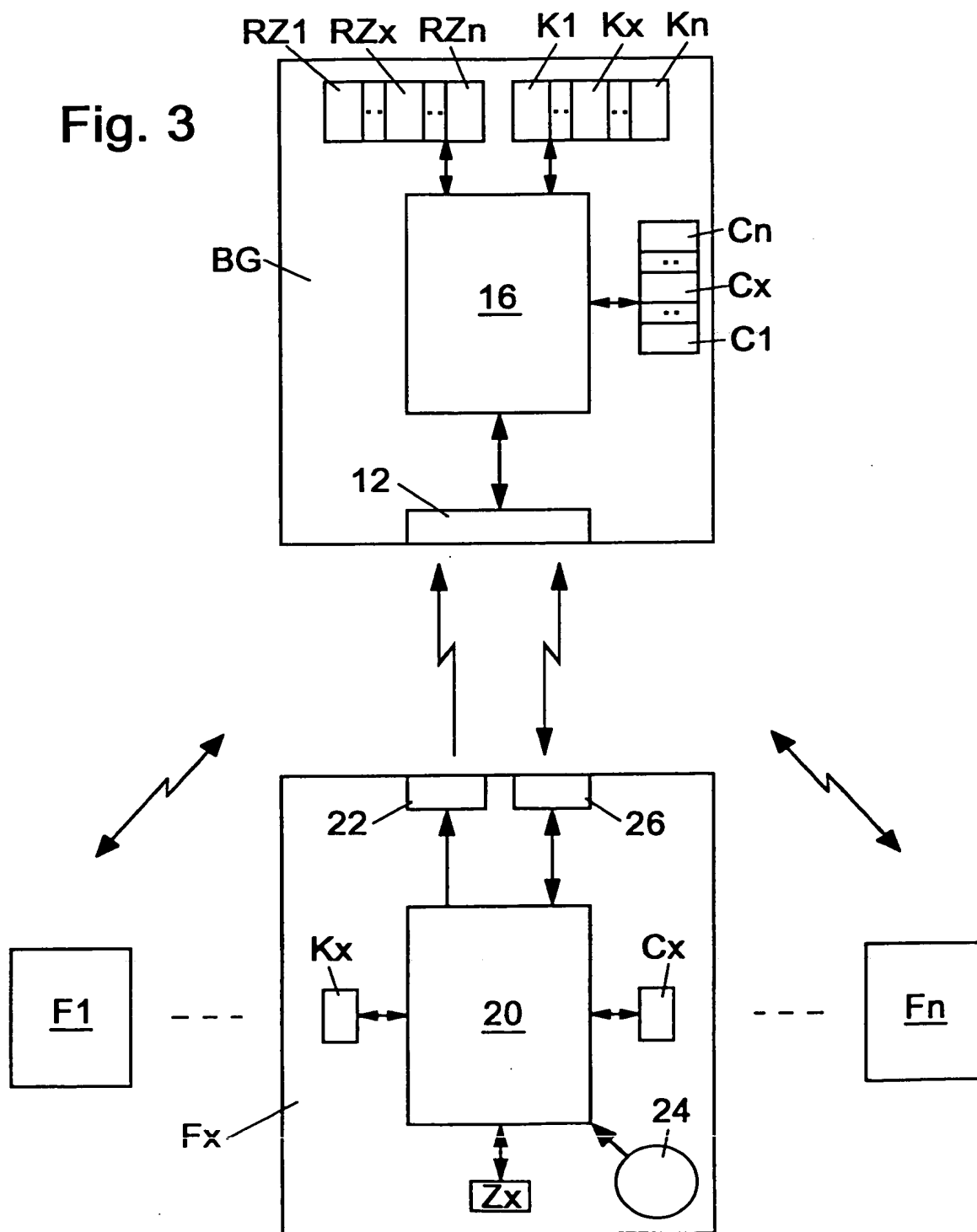


Fig. 4

